UNMASKED

CYBRARY.IT

TAKING THE MYSTERY OUT OF CYBER SECURITY

MARCH 2018 | EDITION 2

IN THIS ISSUE

EDITOR'S NOTE

We know that Cybrary users love to learn on the go. We also know that for awhile there was an issue with our mobile app which we had been working to resolve. At last, we have a fix!

For those of you who haven't updated your Cybrary app, please download the update now. In some cases, you may need to uninstall the current version and re-download it all together.

Those who have never used the mobile app before, we encourage you to do so! The app is available for both iOS and Android, allowing you to watch courses, read articles, and earn Certificates of Completion from the palm of your hand. **Download the mobile app here.**

Olivia Lynch **(@Cybrary_Olivia)** is the Marketing Manager at Cybrary. Like many of you, she is just getting her toes wet in the field of cyber security. A firm believer that the pen is mightier than the sword, Olivia considers corny puns and an honest voice essential to any worthwhile blog.

CYBER SECURITY NEWS

#HACKED

The Equifax breach that affected over 145 million people is a distant memory, right? Wrong. The actual number of individuals impacted is around 148 million. This week, Equifax released information that indicates an additional 2.4 million Americans had their data stolen.

When the breach occurred back in 2017, it sent shock waves across the country and left many cyber security experts with even greater concerns over data security. Those affected had their names, social security numbers and even driver's license information compromised, not to mention Equifax's poor response after the breach left people more vulnerable and confused. Equifax said that it has continued to conduct an 'ongoing analysis' during which they found the additional victim's information was stolen. Unlike the initial victims, those recently affected did not have their social security numbers compromised. Equifax said the new victims were not previously identified because their social security numbers were not stolen with their driver's license information.

“The methodology used in the company’s forensic examination of last year’s cybersecurity incident leveraged Social Security Numbers (SSNs) and names as the key data elements to identify who was affected by the cyberattack,” said the company in a statement. Equifax has yet to respond to requests for further comment, so additional information is limited at this point. This additional disclosure has only resurfaced the initial outrage towards the company.

For details on the Equifax hack, read Equifax and Never Look Back (Wrong!)

#EXPLOITS

Just when we thought the ShadowBrokers had given it a rest, new, previously classified NSA information is released. This time, it's a collection of scripts and scanning tools the agency uses to detect other nation-state hackers.

When the Wikileaks scandal first came to the surface about a year ago, the data shared by the ShadowBrokers revealed secret hacking tools and zero-day exploits used by the agency. Now, almost a year later, Hungarian security researchers from CrySyS Lab has now revealed that the NSA dump "doesn't just contain zero-day

"This is not about newly discovered stolen data. It’s about sifting through the previously identified stolen data, analyzing other information in our databases that was not taken by the attackers, and making connections that enabled us to identify additional individuals."
-Paulino do Rego Barros, Jr., interim CEO of Equifax

exploits used to take control of targeted systems, but also include a collection of scripts and scanning tools the agency uses to track operations of hackers from other countries." In a report published by the Intercept, the NSA had a special team known as 'Territorial Dispute' that developed the scripts and tools. These methods were used to scan targeted systems for 'indicators of compromise (IoC) to protect their own operations from getting exposed while trying to discover what foreign threat actors were involved with and what techniques they were using.

For the information gathered, the Territorial Dispute team maintained a database of digital signatures, such as fingerprints and file snippets to track operations. At the time the ShadowBrokers stole the NSA files, it appears they were tracking 45 different state-sponsored groups. CrySyS researchers will be releasing the full details of their findings this week.

"When the NSA hacks machines in Iran, Russia, China and elsewhere, its operators want to know if foreign spies are in the same machines because these hackers can steal NSA tools or spy on NSA activity in the machines. If the other hackers are noisy and reckless, they can also cause the NSA's own operations to get exposed. So based on who else is on a machine, the NSA might decide to withdraw or proceed with extra caution"
-Intercept report

Explore some of the previous exploits released by the ShadowBrokers in this edition of 'UNMASKED'

#VULNERABILITIES

Love the fast speeds of your 4G LTE network? You probably won't love the latest discovery by security researchers which indicates a severe set of vulnerabilities in the 4G LTE protocol.

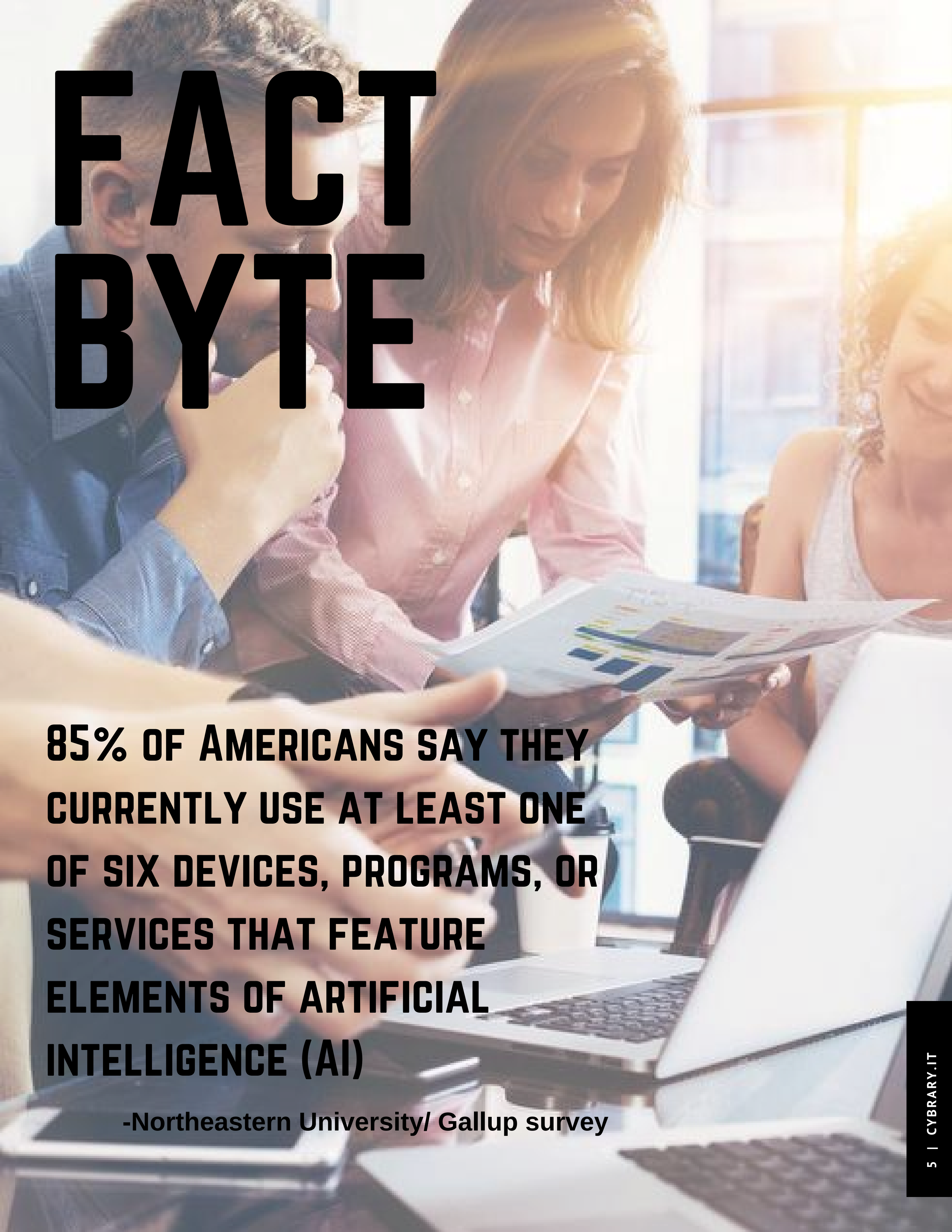
First, let's break down what 4G LTE means for context. 4G means the 4th generation of data technology for cellular networks. LTE stands for Long Term Evolution and is a technical process for high-speed data for mobile devices. The recently discovered vulnerabilities could be exploited to spy on calls, texts, send fake emergency alerts, spoof location, and knock devices entirely offline. In the research paper published by Purdue University and the University of Iowa describes 10 cyber attacks against 4G LTE. These attacks leverage design weaknesses in 3 protocol procedures of the network known as attach, detach, and paging. According to an article from The Hacker News, the researchers employed a systematic model-based adversarial testing approach, which they called LTEInspector and tested 8 out of 10 attacks in a read testbed using SIM cards from four large US carriers.

Of the attacks, most worrisome is the authentication relay attack which allows a hacker to connect to a 4G LTE network by impersonating a victim's phone number without any legitimate credentials. At this time,

researchers do not plan to release proof-of-concept code for these attacks until the flaws are fixed. There are some possible defenses against the observed attacks but, researchers stated: "retrospectively adding security into an existing protocol without breaking backward compatibility often yields band-aid-like-solutions which do not hold up under extreme scrutiny." This discovery continues to surface concerns about the security of cell standards.

Curious about mobile hacking? Watch this video for a better understanding.

"AUsing LTEInspector, we obtained the intuition of an attack which enables an adversary to possibly hijack a cellular device’s paging channel with which it can not only stop notifications (e.g., call, SMS) to reach the device but also can inject fabricated messages resulting in multiple implications including energy depletion and activity profiling"
-researchers



FACT BYTE

85% of Americans say they currently use at least one of six devices, programs, or services that feature elements of artificial intelligence (AI)

-Northeastern University/ Gallup survey

MEET THE CYBRARIAN

Dr. Mansur Hasib

2017 Cybersecurity People’s Choice Award and 2017 Information Governance Expert of the Year Award winner, Dr. Mansur Hasib is the only cybersecurity and healthcare leader, author, speaker, and media commentator in the world with 12 years’ experience as Chief Information Officer, a Doctor of Science in Cybersecurity (IA), who holds the prestigious CISSP, PMP, and CPHIMS certifications.

His course **'Essentials of Cybersecurity Leadership'** was recently added to Cybrary and covers digital leadership and cybersecurity strategy.

START COURSE

TEACH ON CYBRARY

Intro to Bro Scripting

BRICATA

Bricata supplies network cybersecurity solutions that help organizations to harness the power of complete network visibility to detect, hunt, and prevent threats with the only platform that integrates signature inspection, anomaly detection, and malware conviction engine.

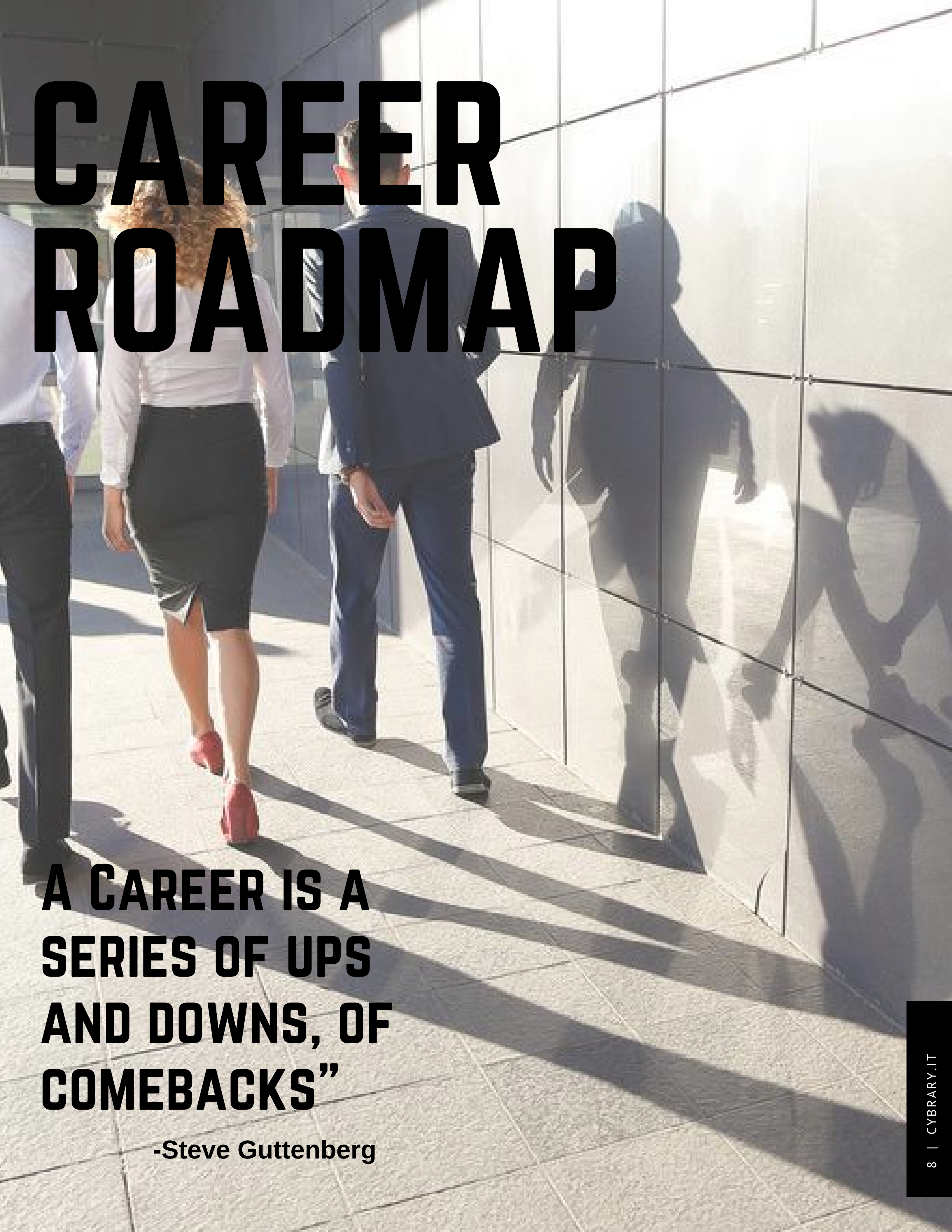
Get Started

Intro to Wireshark Virtual Lab

Practice Labs

The Introduction to Wireshark Virtual Lab will prepare you to properly utilize Wireshark for network troubleshooting, analysis, software and communications protocol development, and education. Having the skills to capture and analyze packets can help you cut to the chase to find out what is really happening on your networks.

Dive In



CAREER ROADMAP

A Career is a series of ups and downs, of comebacks”

-Steve Guttenberg

HOW TO SECURE YOUR SOCIAL MEDIA ACCOUNTS

“Social media represents the largest modern threat vector: it’s got more connectivity (billions of people), it’s more trusted (everyone is your friend) and it’s less visibility (simply by it’s nature) than any other communication or business platform. Security teams need to join their sales, marketing and customer success groups in the digital era, follow social media security best practices and implement risk monitoring and remediation technology around social media to secure their organization’s future.”

Continue Reading

Start Security+ Course

Penetration Tester

Required Knowledge & Skills

Follow the track of an industry leader's job description. Click the buttons below to view courses and supplemental materials that will put you on the path to this career

Assess the state of the network, computer systems, and servers	▶	Network Security Tools
Create trend and correlation analysis and scenario forecasting	▶	Threat Intel
Break into a network using various hacking tools and operating systems	▶	Certified Ethical Hacker
Analyze an organization's security policies and procedures	▶	CASP
Capable of designing their own testing methods	▶	Advanced Pentesting

Career Path Beta Program

Cybrary Career Paths is a new program with the main goal of accelerating your journey to a successful technical career by providing training for technical positions with industry leaders like Cognizant.

Apply Today

INSIDE CYBRARY

RYAN COREY, CEO OF CYBRARY, ON TRAINING IT PROFESSIONALS TO DEFEND AGAINST CYBERATTACKS

“As the threat surfaces expand every day, we’re doing our best to keep up with it by training the next generation of cybersecurity professionals to tackle the threats head-on.”

Cybrary wants to revolutionize cybersecurity and IT learning by making the best training curriculum available, for free, forever.

Read the Full Post

Start a Course